REMARKS

Preliminarily, applicants note that the claims as rejected in the July 22, 2010, Office Action ("Office Action") appear to be the ones on record prior to the filing of a Supplemental Amendment filed July 20, 2010. In this regard, the Office Action states that it is in response to a Communication filed on April 30, 2010. Regardless, presumably the Supplemental Amendment claims have now been entered. This response was prepared based on this presumption. Also, it is applicants' understanding, which was confirmed via a telephone conversation between the undersigned attorney and the Examiner shortly after the Office Action was received, that the statement in paragraph 6 on page 9 of the Office Action that is was a final Office Action is in error. Rather, the Office Action, is a non-final Office Action as stated in the status portion of the form PTOL-326 included in the Office Action.

Turning now to the substance of the Office Action, the Office Action ("Office Action") rejected Claims 1-3 under 35 U.S.C. § 103(a) as being unpatentable in view of the teachings of U.S. Patent Application Publication No. 2003/0214779 ("Socolofsky") taken in view of the teachings of U.S. Patent Application Publication No. 2003/0005336 ("Poo"), and taken further in view of the teachings of U.S. Patent Application Publication No. 2002/0084056 ("DeAnna"). Claims 5-6 were rejected under 35 U.S.C. § 103(a) as being unpatentable in view of the teachings of Socolofsky, Poo, and DeAnna taken further in view of the teachings of U.S. Patent Application Publication No. 2003/0157959 ("Makela"). Finally, Claim 4 was rejected under 35 U.S.C. § 103(a) as being unpatentable taken in view of the teachings of Socolofsky, Poo, and DeAnna taken further in view of the teachings of U.S. Patent Application Publication No. 2002/0186838 ("Brandys"). Applicants respectfully disagree.

Prior to discussing in detail why applicants believe that all of the claims in this application are patentable in view of the teachings of the cited and applied references, a brief description of the disclosed subject matter and brief descriptions of the teachings of the cited and applied references are provided. The following discussions of the disclosed subject matter and the cited and applied references are not provided to define the scope or interpretation of any of the claims of this application. Instead, these discussions are provided solely to assist the U.S. Patent and Trademark Office in recognizing the differences between the pending claims and the cited references, and should not be construed as limiting on the disclosed subject matter.

Disclosed Subject Matter

A portable personal server device suitable for functioning as a server when connected to an external network is disclosed. The portable personal server device comprises a local server, a network server, memory, a messaging API, an individual authenticator, and a control. The local server processes data between the portable personal server device and a communication terminal equipped with a local network connector suitable for connection to the portable personal server device. The network server processes data between the portable personal server device and an external device through an external network connected to the communication terminal by the communication terminal's local network connector. The memory stores an operating system for controlling the data processing operations of the local server and the network server. The memory also stores application services executable by the portable personal server device. The memory also stores user specific data. The operating system loads the application services into other memory locations on demand during execution. The messaging API allows the communication terminal and other goods and services devices returned to the communication terminal to discover and use the application services and access the user-specific data stored in memory as if the application services and data were stored in the communication terminal or another device networked to the communication terminal. The messaging API also facilitates secure communication between the communication terminal and the portable personal server device and between the portable personal server device and other devices networked to the communication terminal. The individual authenticator authenticates an individual based on biometric information, and the control makes the local server and the network server usable only when the individual is authenticated.

The disclosed personal portable server device has a number of advantages. It allows a user to carry his/her own data and unique applications and make them available to others securely over a network connection via any communications terminal, such as a PC. This is both unique and novel. Before the disclosed subject matter was developed, a portable personal server device had not been conceived. More specifically, until the disclosed subject matter was created, no one had developed a personal portable server device combining the unique and novel approaches described in the current application.

The disclosed portable personal server device can be used to implement a number of different applications that provide application services on behalf of its owner and independent of any other server infrastructure such as access to an authentication server. Because the portable personal service device includes its own processing and storage capability, the portable personal server device can provide these functions without the need for any other Internet server. Some examples were described in the response from in this application filed on April 30, 2010. Another one is described below.

- A *virtual private network proxy and firewall service* that provides a highly secure encrypted communication channel to a secure network server without revealing that server's address or connection information. A lead auditor may use such service to access the auditor's network from within a corporate network operated by the corporation that the auditor is auditing. After biometric authentication, the auditor may also allow his/her audit team members (authenticated by their own portable personal server devices) to also use the auditor's secure communication channel, too. In this example, the auditor's portable personal server device acts as a proxy server.

Because the portable personal server device relies on a communication terminal, the portable personal server device (i) does not need to have any user input or output mechanism such as a keyboard or display; (ii) uses a local network connection, such as a USB connection; and (iii) does not need sophisticated network interfaces. Therefore, the device can be very small, even smaller than today's smallest smart phones. When a user wants to access the data and applications on his portable personal server device, he uses a communication terminal, which can have large screens, unique input devices (such as touch screens, mouse or keyboard), and powerful CPU processing capabilities to access the data and the applications. If an owner wants to share his data and applications with others, such as team members, for example, the user can use the sophisticated wired, wireless, or cellular network interfaces of any communication terminal of the user's choice and the communication terminal will relay any communication between the team members and the portable personal server device.

Even though some aspects of these application services might have been implemented on state of the art hardware devices, the unique combination of application and security services of the portable personal server device allow for many new combinations of applications.

U.S. Patent Application Publication No. 2003/0214779 (Socolofsky)

Socolofsky describes a server for sharing multimedia information (images) across a network to multiple client personal computers (PCs). Specifically, visual data, such as Web pages with pictures and video, are shared and displayed with the help of a Web browser application to the client PCs. While Socolofsky does include server functionality, the server described by Socolofsky is very traditional with a hard disk, separate power supply, and an Ethernet network interface.

Socolofsky discloses a PC which can only connect to the server device via the server's Ethernet network interface and an additional device (either a USB/Ethernet adapter or a router). Contrary to statements made in the Office Action, Socolofsky does not disclose both local and network server functions. The disclosed portable personal server device is connectable directly by a communication terminal without the need of any additional device. Socolofsky's server requires either a network adapter or a router to connect to a PC.

In Figure 7, paragraph [0037], Socolofsky discloses a PC connected to a server through a USB/Ethernet adapter and a crossover Ethernet cable connection for server configuration. In this configuration, the server cannot connect to other devices over the network. As a result, this configuration is very different from the configuration shown in FIGURE 1 of this application in that it does not provide a network server function.

In Figure 8, paragraph [0038], Socolofsky discloses a PC connected to a server through a router. The router also allows any number of other devices on the home network or Internet to access the server directly. This configuration is very different from the claimed subject matter in that the claimed portable personal server device connects to the communication terminal (through a local network connection such as a simple USB connection without any type of Ethernet network adapter). It is the communication terminal that then makes the connection to an external network. Unlike Socolofsky's Figure 8, the communication terminal relays all communication between any device on the external network and the portable personal server device.

Further, as recognized in the Office Action, Socolofsky does not disclose a messaging API directed to performing the recited API functions. Also, as recognized in the Office Action, Socolofsky does not disclose an individual authenticator for authenticating an individual based on biometric information nor a control that makes a local server and a network server usable only when an individual is authenticated by an individual authenticator.

The purpose of Socolofsky's server is to share media through a Web server. In contrast, the disclosed subject matter provides a way to transport, secure, and share personal data as well as provide application functions in a small, portable personal server device.

U.S. Patent Application Publication No. 2003/0005336 (Poo)

Poo discloses a portable device having biometric-based authentication capabilities such as a fingerprint reader. Fingerprints can be registered and stored in an encrypted format and later used for authentication to access an external restricted resource such as a network server. Other than this disclosure, Poo has little, if any, relevance to the disclosed subject matter.

Remarks in the Office Action state that it would be obvious to combine the authentication capabilities of Poo with the server capabilities of Socolofsky. The purported motivation for doing so would have been to provide a secured access control mechanism for protection against unauthorized access. Applicants respectfully disagree. Socolofsky's server is configured to host a Web site for showing images (multimedia content) posted to the Web site across the network. There is no indication in Socolofsky that the multimedia content is confidential and, as a result, needs protection from unauthorized access. Only the Office Action comments, which are clearly based on prohibited hindsight, conclude that there is a need to protect Socolofsky's multimedia content from unauthorized access.

U.S. Patent Application Publication No. 2002/0084056 (DeAnna)

DeAnna does not disclose a portable personal service device that allows a user to carry the user's own data and unique applications with him/her. Rather, DeAnna discloses an application server system that includes a messaging API for use on portable or embedded devices such as PDAs or smart phones and how such application server technology can be used to build enterprise-distributed applications. DeAnna's system allows, for example, medics in the field to use PDAs and smart phones to access corporate distributed resources (Figure 3E). DeAnna's system allows a corporate IT administrator to use application servers to manage the applications available on such devices (Figure 2C). The DeAnna system clearly distinguishes between client devices (paragraph [0049]) and server devices (paragraph [0048]), which includes traditional enterprise servers such as the Decision Flow Services (paragraph [0082]) using J2EE running within a BEA WebLogic server.

The disclosed portable personal server device requires no user input/output mechanism. As a result, it is very different from the portable devices disclosed by DeAnna, which have a display and some type of user input device, such as a keyboard. The portable devices disclosed by DeAnna connect directly to the (wireless) network rather than through a communication terminal. DeAnna does not disclose any way of pairing a portable device with a more capable PC, which is allowed by the communication terminal connection disclosed and recited in the claims of this application. Further, the portable devices disclosed by DeAnna do not distinguish between local and network servers.

In paragraph [0121], DeAnna neither discloses how a biometric application would be used nor any biometric usage control. Instead, DeAnna relies on traditional enterprise security services, which require a user to enter a userid and a password, both of which are verified against a central LDAP enterprise server. The portable personal server device disclosed in this application differs from DeAnna's traditional enterprise server infrastructure because the portable personal server device is self-contained; for example, user authentication is done by comparing the fingerprint entry with the locally stored, previously registered information. Therefore the disclosed portable personal server device can be used securely even on a plane, submarine, or battlefield standalone or on an *ad hoc* network where any centralized authentication infrastructure may not be available.

U.S. Patent Application Publication No. 2003/0157959 (Makela)

Makela describes a server that is used to provide additional data storage for other small portable devices and also allows those portable devices to share data. Even though Makela's technology appears to be somewhat similar in nature to the disclosed subject matter, there are substantial differences both with respect to structure and function. With regard to function, Makela's server is specifically intended for use as a **multi-user** device. In contrast, the disclosed subject matter is specifically targeted to store and manage a **single** person's data and unique applications. The owner of the disclosed device is expected to take the device along as he/she travels. The owner may specifically allow others to access his/her data and applications via biometric authentication. The device is therefore called *personal* server device. This approach is unique and novel.

With respect to structure, Makela does not disclose local and network servers that perform the functions described above, or a memory for storing and carrying out the functions recited above. Most importantly, Makela does not disclose a messaging API for carrying out the functions described above. And, of course, Makela does not disclose an authenticator for authenticating an individual based on biometric information and/or a control that makes a local server and a network server only usable when an individual is authenticated.

U.S. Patent Application Publication No. 2002/0186838 (Brandys)

Brandys is directed to a system and method of user and data authentication. The data verification method and system employ authenticating biometric information to create a digital signature. More specifically, biometric data is analyzed and carries a random number generator that creates a public key and a private key. The private key is stored in a tamper-resistant component; the public key is transmitted to an external device, such as a computer. Thereafter, messages are digitally signed using the private key subsequent to verifying the biometric information that is provided by the user. Brandys does not disclose a portable personal server device, much less a portable personal server device containing the structural elements and/or functions described above. Brandys discloses using encryption for digitally signing a message as a way to authenticate the message, but does not disclose using encryption for other purposes such as preventing eavesdropping of communications or privacy of stored information as described above.

Argument

As amended, Claim 1 reads as follows:

> 1. A portable personal server device suitable for functioning as a server when connected to an external network, the portable personal server device comprising:
>
> a local server for processing data between the portable personal server device and a communication terminal equipped with a local network connector suitable for connection to the portable personal server device;
>
> a network server for processing data between the portable personal server device and an external device through an external network connected to the communication terminal by said communication terminal's local network connector;
>
> memory for storing an operating system for controlling the data processing operations of the local server and the network server, the memory also storing application services executable by the portable personal server device, the memory also storing user specific data, the operating system loading the application services into other memory locations on demand during execution;
>
> a messaging API for (i) allowing the communication terminal and other devices networked to the communication terminal to discover and use the application services and access the user specific data stored in memory as if the application services and data were stored in the communications terminal or another device networked to the communication terminal and (ii) facilitating secure communication between the communication terminal and the portable personal server

> device and between the portable personal server device and other devices networked to the communication terminal;
>
> an individual authenticator for authenticating an individual based on biometric information; and
>
> a control that makes said local server and said network server useable only when authenticated by said individual authenticator.

The important underlying concept of the subject matter recited in Claim 1 is that the portable personal server device (i) allows a user to carry his/her own data and unique applications and, (ii) when connected to any communications terminal (such as a PC) that is connected to an external network, make such data and applications available to others in a secure manner. This concept is clearly not taught or even remotely suggested by Socolofsky, Poo, and DeAnna taken alone or in any reasonable combination. Only prohibited hindsight reasoning based on the current application, not the teachings of the references, provide support for the rejection of Claim 1. Socolofsky describes a portable server. Poo describes a device that employs biometric authentication to control access to restricted resources. DeAnna allegedly discloses a messaging API that performs the functions recited in Claim 1. However, none of Socolofsky, Poo, or DeAnna teaches, describes, or suggests the underlying concept of the claimed invention. This concept is both unique and novel. The language of Claim 1 clearly recites new and unique subject matter that covers the concept in a way that is patentably distinguishable over the teachings of the references.

More specifically, applicants respectfully submit that the subject matter of Claim 1 is clearly allowable in view of the teachings of Socolofsky, Poo, and DeAnna. Neither reference, taken alone or in combination, teaches all of the subject matter recited in Claim 1:

1. None of the references teach the concept of a **communication terminal** which relays information between an external network and a simple server device providing **local and network server** functions. By offloading the user input and output, some of the processing, and network connectivity functions to the

communication terminal, the portable personal server device can be very small and portable and still take advantage of ever increasingly powerful PCs.

2. None of the references teach a **biometric usage control** which, when the owner has authenticated himself, allows the owner and any number of users over the network to gain access to the owner's restricted resources contained in the portable personal server device; Poo teaches biometric authentication only for a single individual to gain access to a restricted resource.

Further, applicants respectfully submit that there is no basis disclosed in any of the three references (Socolofsky, Poo, and DeAnna) applied to Claim 1 as to why the subject matter of the references should be combined in any manner. Only the current application suggests any combination. More specifically, as noted above, there is simply no basis, absent the present disclosure, for concluding that it would have been obvious to a person of ordinary skill at the time this invention was made to combine the biometric authentication disclosure of Poo with the portable server disclosure of Socolofsky. Socolofsky is directed to storing large amounts of multi-media, such as movies, TV shows, etc. Nothing in Socolofsky indicates that the access to the stored material should be restricted in any manner. Thus, there is no need to use biometric or any other means to prohibit access.

Similarly, there is no need to include a messaging API in Socolofsky. In this regard, the Office Action states that the motivation included an API, such as that disclose by DeAnna, in Socolofsky would be to better facilitate better interaction between different programs in the server. Applicants disagree. Even if the API disclosed by DeAnna performed the functions recited in Claim 1, which applicants deny, there is no perceived need in Socolofsky for such an API.

As a result, as noted above, applicants submit that the rejection of Claim 1 based on the combination of these three references is using impermissible hindsight, not the teachings of the cited references to conclude that the claimed invention is unpatentable. As a result, applicants request that the rejection of Claim 1 be withdrawn and that Claim 1 be allowed.

Since all of the remaining claims in this application (Claims 2–6) are directly or indirectly dependent upon Claim 1 and since none of the other cited and applied references (Makela and Brandys) teaches the subject matter missing from Socolofsky, Poo, and DeAnna, these claims are submitted to be allowable for at least the same reason that Claim 1 is allowable. Further, these claims are submitted to be allowable for additional reasons. For example, while Brandys does disclose data encryption and data encryption using biometric information, again, applicants respectfully submit that there is no basis in Socolofsky, Poo, DeAnna, or Brandys to conclude that it would be obvious to combine the subject matter of these references. Only the present disclosure suggests the use of biometric information to provide encryption in a portable personal server device of the type recited in Claim 1. As a result, applicants respectfully submit that Claim 4 is clearly allowable for reasons in addition to the reasons why the claims from which these claims depend are allowable. Likewise, with respect to Claims 5 and 6, there is simply no basis in Socolofsky, Poo, and DeAnna, or Makela to conclude that it would be obvious to combine the teachings of these references in any manner, much less the manner recited in Claims 5 and 6, when the subject matter of these claims is considered in combination with subject matter of the claims from which these claims depend.

In view of the foregoing amendments and remarks, applicants respectfully submit that all of the claims in this application are allowable. Consequently, early and favorable action allowing these claims and passing this application to issue are respectfully solicited.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^PLLC

Gary S. Kindness

Gary S. Kindness
Registration No. 22,178
Direct Dial No. 206.695.1702

GSK:mgp